(b) Deny access to the OCS facility, except to those responding to an emergency;

(c) Evacuate the OCS facility in case of security threats or breaches of security; and

(d) Report security incidents as required in § 101.305 of this subchapter;

(e) Brief all OCS facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(f) Secure non-critical operations in order to focus response on critical operations.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003]

Subpart C—Outer Continental Shelf (OCS) Facility Security Assessment (FSA)

§ 106.300 General.

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.

(b) A single FSA may be performed and applied to more than one OCS facility to the extent they share physical characteristics, location, and operations.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

(1) Knowledge of current and anticipated security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Recognition of techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on structures and essential services;

(7) OCS facility security requirements;

(8) OCS facility and vessel interface business practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine or civil engineering; and

(13) OCS facility and vessel operations.

§ 106.305 Facility Security Assessment (FSA) requirements.

(a) *Background.* The OCS facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the OCS facility, including:

(i) The location of each access point to the OCS facility;

(ii) The number, reliability, and security duties of OCS facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The essential maintenance equipment and storage areas;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring OCS facility and vessel personnel;

(4) Procedures for controlling keys and other access prevention systems;

(5) Response capability for security incidents;

(6) Threat assessments, including the purpose and methodology of the assessment, for the OCS facility's location;

(7) Previous reports on security needs; and

(8) Any other existing security procedures and systems, equipment, communications, and OCS facility personnel.

(b) *On-scene survey.* The OCS facility owner or operator must ensure that an

on-scene survey of each OCS facility is conducted. The on-scene survey examines and evaluates existing OCS facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) *Analysis and recommendations.* In conducting the FSA, the OCS owner or operator must ensure that the Company Security Officer (CSO) analyzes the OCS facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey, including but not limited to:

(i) Access to the OCS facility;

(ii) Structural integrity of the OCS facility;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to essential services;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Existing agreements with private security companies;

(vii) Any conflicting policies between safety and security measures and procedures;

(viii) Any conflicting OCS facility operations and security duty assignments;

(ix) Any deficiencies identified during daily operations or training and drills; and

(x) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits.

(2) Possible security threats, including but not limited to:

(i) Damage to or destruction of the OCS facility or of a vessel adjacent to the OCS facility;

(ii) Smuggling dangerous substances and devices;

(iii) Use of a vessel interfacing with the OCS facility to carry those intending to cause a security incident and their equipment;

(iv) Use of a vessel interfacing with the OCS facility as a weapon or as a means to cause damage or destruction; and

(v) Effects of a nuclear, biological, radiological, explosive, or chemical attack to the OCS facility's shoreside support system;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the OCS facility's infrastructure, policies and procedures;

(5) Any particular aspects of the OCS facility, including the vessels that interface with the OCS facility, which make it likely to be the target of an attack;

(6) Likely consequences, in terms of loss of life, damage to property, or economic disruption, of an attack on or at the OCS facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) *FSA Report.* (1) The OCS facility owner or operator must ensure that a written FSA report is prepared and included as a part of the FSP. The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability;

(v) A list of the key OCS facility operations that are important to protect; and

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the OCS facility.

(2) A FSA report must describe the following elements within the OCS facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Essential services.

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) OCS facility personnel;

(ii) Visitors, vendors, repair technicians, vessel personnel, etc.;

(iii) OCS facility stores;

(iv) Any security communication and surveillance systems; and

(v) Any other security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between personnel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key OCS facility measures and operations, including—

(i) Ensuring performance of all security duties;

(ii) Controlling access to the OCS facility through the use of identification systems or otherwise;

(iii) Controlling the embarkation of OCS facility personnel and other persons and their effects (including personal effects and baggage, whether accompanied or unaccompanied);

(iv) Supervising the delivery of stores and industrial supplies;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the OCS facility; and

(vii) The ready availability of security communications, information, and equipment.

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan (FSP) required in § 106.410 of this part.

(b) An OCS facility owner or operator may generate and submit a report that contains the FSA for more than one OCS facility subject to this part, to the extent that they share similarities in physical characteristics, location and operations.

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

§ 106.400 General.

(a) The OCS facility owner or operator must ensure the FSO develops and implements a Facility Security Plan (FSP) for each OCS facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Facility Security Assessment (FSA);

(4) Must describe security measures for each MARSEC Level; and

(5) May cover more than one OCS facility to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the cognizant District Commander.

(b) The FSP must be submitted for approval to the cognizant District Commander in a written or electronic format in a manner prescribed by the cognizant District Commander.

(c) The FSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.